

# LAB SAFETY SUPPLY

Lab Safety Supply, Inc.

Phone: (608) 754-2345

FAX: 608-754-1806

TWX: 910-288-2921

DOCKET FILE COPY ORIGINAL

January 14, 1994

RECEIVED

JAN 19 1994

FCC - MAIL ROOM

Mr William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems security and I am aware that although I may reduce the risk, no matter how many steps I take to secure my system, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by Interexchange Carriers, Local Exchange Carriers and Computer Processing Equipment vendors. The legal obligations of the IXC's, LEC's, and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABCDE

*Diag*  
0

MAILING ADDRESS  
P.O. Box 1368  
Janesville, WI 53547-1368

PLANT LOCATION  
401 S. Wright Road  
Janesville, WI 53546

Mr. William Canton

Page 2

January 14, 1994

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

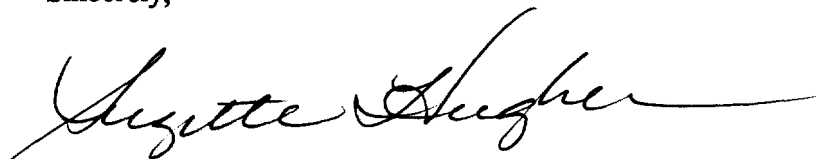
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the ;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendors(s), LEC(s), and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in cursive script, appearing to read "Suzanne Hughes", with a long horizontal flourish extending to the right.

January 11, 1994

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABCDE

*Orig.*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in cursive script, appearing to read "Rick House".



9801 Washingtonian Boulevard  
Gaithersburg, Maryland 20878-5356  
(301) 417-3000

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 14, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.



**Bechtel Power Corporation** A unit of Bechtel Corporation

No. of Copies rec'd One  
List ABCDE

Mr. William F. Canton  
January 14, 1994  
Page 2 of 2

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitable distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Jane Reber  
Manager of Telephone Services



Information Services / Telecommunications  
Metropolitan Park West  
1100 Olive Way, Suite 1800  
Seattle, WA 98101-1448  
REG. No (206) 287-2360

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1993

FCC MAIL ROOM

January 10, 1993

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd One  
List ABCDE

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

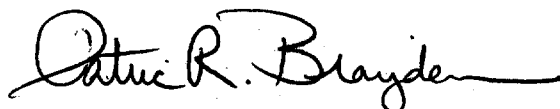
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



MANAGER, VOICE TECHNOLOGY  
GROUP HEALTH COOPERATIVE OF PUGET SOUND





DOCKET FILE COPY ORIGINAL

Cloday Corporation  
312 Walnut Street  
Suite 1600  
Cincinnati, Ohio 45202-4036 USA  
(513) 381-4800 • Fax (513) 762-3984

An Instrument Systems Company

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications system, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my system, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems.

While the programs offered by IXCs, such as AT&T NetProtect, have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking into

No. of Copies rec'd  
List ABCDE

*Orig.*

Mr. Canton  
January 11, 1994  
Page Two

systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there would not be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

  
Allyson Gray-Stacey  
Manager Office Services

**MHG**  
**MEMORIAL HOSPITAL**  
**AT GULFPORT**

*The Health Care Center of South Mississippi*

DOCKET FILE COPY ORIGINAL

**RECEIVED**

**JAN 19 1994**

**FCC MAIL ROOM**

January 13, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE's vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

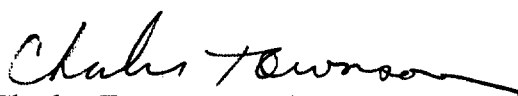
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with a adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

  
Charles Townson, FACHE  
Director Information Systems



## Allendale Insurance

Allendale Mutual Insurance Company  
Allendale Park, P.O. Box 7500  
Johnston, Rhode Island 02919-0500  
Tel. (401) 275-3000

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 12, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC DOCKET 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunication professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking. I walk a tight rope wondering when my company's communications will be hacked, as they say, there are only two types of companies, THOSE THAT WERE HACKED AND THOSE THAT WILL BE!

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100%. If the equipment and services provided by the LECs, IXC's, CPE's, are also open for Toll Fraud, shouldn't they be held as responsible as the PBX owner for all costs? Perhaps if they had a legal obligation to warn customers of know weaknesses and be held liable for half of the monetary value, they might have a real incentive to fight a full battle against hackers.

It takes me about an hour to read through all of the reports from the monitoring devices I have in place that will alert me of hacking. In addition to the cost of these monitors, production time lost is considered a major loss.

We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Sincerely,

*Wanda J. Agresti*

WANDA J. Agresti

No. of Copies rec'd  
List ABCDE

*Agresti*

150 years



IF IT'S BORDEN-IT'S  
GOT TO BE GOOD

DOCKET FILE COPY ORIGINAL

BORDEN, INC.

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 13, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard, MCI Detect and AT&T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. ALL CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed

No. of Copies rec'd  
List ABCDE

180 EAST BROAD STREET  
COLUMBUS, OHIO 43215  
TELEPHONE: 614/225-4000

at the time of purchase and at installation. All customer passwords should be changed or created at installation. All customers should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

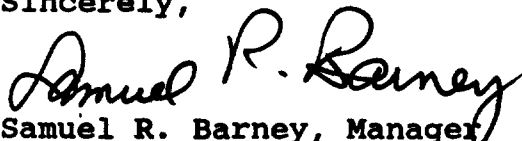
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

  
Samuel R. Barney, Manager  
Voice Network



# BOARD OF EDUCATION OF THE CITY OF NEW YORK

RAMON C. CORTINES, Chancellor

OFFICE OF THE CHANCELLOR

110 LIVINGSTON STREET - BROOKLYN, NY 11201

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard, MCI Detect, and AT&T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risk of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change, schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

No. of Copies rec'd  
List ABCDE

*Orig.*



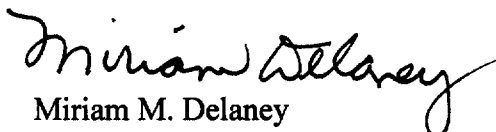
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owners to secure their equipment
- CPE vendors to warn customers of specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one more parties then the financial loss should be equitable distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitably distributed among CPE owners, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in cursive script, reading "Miriam M. Delaney".

Miriam M. Delaney  
Director of Telecommunications



## W. L. GORE &amp; ASSOCIATES, INC.

1901 BARKSDALE ROAD • P.O. BOX 9236 • NEWARK, DELAWARE 19714-9236  
 PHONE: 302/368-3700 • FAX: 302/738-5993

ELECTRONIC PRODUCTS DIVISION

January 10, 1994

Mr. William F. Canton  
 Acting Secretary  
 Federal Communications Commission  
 1919 M Street NW  
 Washington, D.C. 20554

RE: CC Docket 93-292

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services, and equipment provided IXCs, LECs, and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll

No. of Copies rec'd Orig.  
 List ABCDE

fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

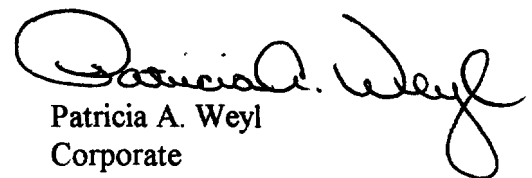
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to comprise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the system and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on these terrible problem.

Sincerely,

  
Patricia A. Weyl  
Corporate  
Telecommunication  
Manager

PAW/saw

**Beaumont**William Beaumont Hospital  
Royal Oak**RECEIVED****JAN 19 1994****FCC MAIL ROOM**

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554**RE: CC DOCKET NO. 93-292**

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligation of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard<sup>™</sup>, MCI Detect<sup>™</sup>, and AT&T Netprotect<sup>™</sup>) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offering. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be

*Orig.*

changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encourage to offer security related hardware and software in the price of their systems.

The provisions outline in the NPRM are fair and equitable. Share liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment.
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services.

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s), IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Kathy Grady  
Systems Manager

cc: Stacey Petsikas

C:\dt\wp\misc\cantor



ROCKET FILE COPY ORIGINAL

Schering-Plough Corporation  
3030 Jackson Avenue  
P. O. Box 377  
Memphis, TN 38151-0001 U.S.A.

Telephone 901/320-2011  
Telex 53861

**RECEIVED**

**JAN 19 1994**

**FCC MAIL ROOM**

**January 12, 1994**

**Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554**

**Re: CC Docket no. 93-292**

**Dear Mr. Canton:**

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs, and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All

No. of Copies rec'd  
List ABCDE

*Aug.*

login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,

*W. Dale Mathis*  
W. Dale Mathis

January 11, 1994

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABCDE

*Orig.*



CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

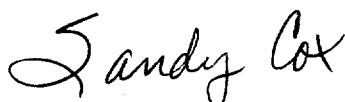
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in cursive script that reads "Sandy Cox".

Sandy Cox  
Sr. Telecomm Analyst  
TX Guaranteed Student Loan Corp.